Audit Report

YEAR 2000 POSTURE OF DOD MID-TIER COMPUTER SYSTEMS

Report No. 99-076 February 3, 1999

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: **Year 2000 Posture of DoD Mid-Tier Computer Systems**

B. DATE Report Downloaded From the Internet: **09/02/99**

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):
OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/02/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronym

Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

February 3, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on Year 2000 Posture of DoD Mid-Tier Computer Systems (Report No. 99-076)

We are providing this report for information and use. Because this report contains no findings or recommendations, no written comments were required, and none were received.

Questions on the audit should be directed to Mr. James W. Hutchinson at (703) 604-9060 (DSN 664-9060) or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049). See Appendix D for the planned report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-076
(Project No. 8AS-0050)

February 3, 1999

Year 2000 Posture of DoD Mid-Tier Computer Systems

Executive Summary

Introduction. This report is one of a series of reports that the Inspector General, DoD, is issuing in accordance with an informal partnership with the DoD Chief Information Officer to monitor DoD efforts to address the year 2000 computing challenge.

Objectives. The overall audit objective was to assess whether DoD mid-tier computer systems will operate properly after the year 2000. Specifically, we evaluated efforts taken to ensure that mid-tier computers and associated executive software were year 2000 compliant.

Results. Managers of the 14 mid-tier systems reviewed were actively managing each primary element to achieve year 2000 compliance, and they appropriately reported the year 2000 status of each mission-critical computer system. The major reason that mid-tier systems were appropriately managed and reported was because the primary elements of each system were the responsibility of a single manager. Additionally, Army and Air Force year 2000 reporting guidance specifically requires that Service sub-components track and report each primary element of computer systems. Further, some program managers prudently went beyond existing year 2000 requirements to employ further risk-reduction tactics, such as testing vendor-validated products. Accordingly, for the mid-tier systems reviewed, we judged that the risk of system failure at the turn of the century because of a primary element being overlooked was low.

Management Comments. We provided a draft of this report on December 29, 1998. Because this report contains no findings or recommendations, written comments were not required, and none were received. Therefore, we are publishing this report in final form.

Table of Contents

Background

DoD operates thousands of computer systems, which support every function of the DoD enterprise. Computer systems support DoD strategic and tactical operations such as mobilizing, deploying, and maneuvering forces; gathering and processing intelligence; conducting surveillance; providing security; and operating weapon systems. Computer systems also support core DoD business functions such as financial management, personnel management, health care, contract management, and logistics management.

Because computer systems have typically used two digits to represent the year, the year 2000 (Y2K) is indistinguishable from 1900. As a consequence, computers and associated executive software and application programs that use dates to calculate, compare, and sort could generate incorrect results when working with years after 1999. The potential for computer system failure at the turn of the century is often referred to as the Y2K problem.

During our review, DoD Components were using the June 1998 version 2.0 of the draft DoD Y2K Management Plan as Y2K criteria. The Plan addresses computer systems in general; however, it does not specifically address mid-tier computer systems. The December 1998 version of the DoD Y2K Management Plan also does not specifically address mid-tier computer systems.

DoD Computer Systems. In November 1998, DoD reported to the Office of Management and Budget that 2,642 of its computer systems were mission critical. Among systems defined as mission critical are those that are required to perform DoD or DoD Component-level core functions. Appendix C provides the full definition of mission-critical systems and other technical or uncommon terms used in this report.

Computer systems have three primary elements: the hardware, the executive software, and the application program.

- **Hardware.** Hardware consists of the physical components of a computer system, which include the computer and peripherals such as printers, tape drives, and other data storage devices.

- **Executive Software.** Executive Software is the collective name for all the system software products, including the operating system, that support the application program.

- **Application Program.** An application program is software designed to help people perform a certain type of work. Application programs perform many and various functions, from paying employees to controlling the flight surfaces of aircraft.

Depending on their physical size, computing speed, and processing capabilities, DoD computer systems are generally classified into three loosely bounded categories: mainframe, mid-tier, and personal computer systems.

- Mainframe computers are considered the largest and most powerful class of general-purpose computers. Mainframes are typically housed in a specialized environment that provides for specific temperature, humidity, and electrical power requirements. Mainframes can process several applications concurrently and can simultaneously support hundreds of user terminals. The Defense Information Systems Agency owns most mainframe computers and operates them within consolidated facilities called Megacenters. The Megacenters sell mainframe computer processing services to functional users throughout DoD.

- Mid-tier computers are often called "mini-computers" and are less powerful than mainframes. Mid-tier computers have many of the operational characteristics and capabilities of mainframe computers. Unlike mainframes, mid-tiers do not require a specialized environment and are commonly operated in a typical business office setting. The number of mid-tier computers owned by DoD is not well defined, but it is generally acknowledged to be in the thousands.

Objectives

The overall audit objective was to assess whether DoD mid-tier computer systems will operate properly after the Y2K. We evaluated efforts taken to ensure that mid-tier computers and associated executive software were Y2K compliant. See Appendix A for a discussion of the audit scope and methodology.

Year 2000 Posture of DoD Mid-Tier Computer Systems

Managers of the 14 mid-tier computer systems reviewed during the audit were actively managing each primary element to achieve Y2K compliance, and they appropriately reported the mid-tier systems' Y2K posture. The major reason that mid-tier systems were being appropriately managed and reported was because the primary elements of each system were the responsibility of a single manager. Additionally, Army and Air Force Y2K reporting guidance specifically requires that Service subcomponents track and report each primary element of computer systems. Further, some system managers went beyond existing Y2K requirements to employ further risk-reduction tactics. Accordingly, for the mid-tier systems reviewed, we judged that the risk of system failure at the turn of the century because of a primary element being overlooked was low.

Audit Impetus and Approach

Audit Impetus. DoD Components are required to track their Y2K remediation efforts and periodically report the Y2K status of each mission-critical computer system to the Office of the Secretary of Defense. DoD is required to report its overall Y2K status to the Office of Management and Budget. As described in Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998, DoD inappropriately reported some mainframe computer systems as Y2K compliant. Specifically, DoD reported the application program as compliant even though the associated mainframe computer or executive software was not compliant. DoD requires that each primary element of the computer system be Y2K compliant before the system can legitimately be reported as compliant.

Audit Approach. The audit was to gauge whether managers were considering each primary element of mid-tier computer systems during Y2K remediation efforts and to gauge whether the Y2K status of the systems was being correctly reported. Because DoD functional proponents were developing plans for end-to-end testing, we examined mid-tier computer systems that were likely to be included in testing for two DoD major functional areas: military personnel and transportation. We also reviewed mid-tier computer systems at a DoD Megacenter and assessed Y2K efforts for the Defense Information Infrastructure - Common Operating Environment. In essence, the Common Operating Environment is a standard set of executive software used primarily by the mid-tier computer systems that are operated by the DoD command and control community. Appendix B provides a description of each computer system that we reviewed.

Y2K Management of Mid-Tier Computer Systems

Managers of the mid-tier computer systems were aware of the Y2K status of each system's primary elements and were actively engaged in ensuring the Y2K compliance of each element. Additionally, the program managers accurately reported the Y2K status of each mid-tier system that we reviewed. We believe that the appropriate Y2K management and reporting of mid-tier computer systems is the result of two primary factors: single-system management and detailed Y2K reporting requirements.

Single-System Management. A single organization owned and managed the three primary elements of each mid-tier computer system that we reviewed. A factor contributing to the earlier inappropriate reporting of mainframe computer systems was that different DoD Components owned and reported the Y2K status of different primary elements. The Defense Information Systems Agency owned, controlled, and reported the computer hardware and executive software, and the Military Departments and other Defense agencies owned and reported the application programs. For almost all the mid-tier systems that we reviewed, a single organization owned and managed the three primary system elements.

Y2K Reporting Requirements. Detailed reporting requirements also contributed to effective computer system oversight. The Army and the Air Force require reporting of mid-tier system details in their respective Y2K databases. The database fields require Service subcomponents to track and report the Y2K status for the system application, hardware, and executive software. In addition, the databases contain fields that address detailed software and hardware information, such as version number, type, and vendor.

The Navy did not require detailed reporting of each primary mid-tier system element in its Y2K database; however, the Navy tracked hardware and software at the subcomponent level. The previous Navy Y2K database, the Defense Integration Support Tools database, tracked some mid-tier detail information, such as hardware platform. However, the Defense Integration Support Tools database was terminated for Y2K tracking in March 1998, and the Navy quickly developed its own database that did not require details related to each primary system element.

Risk Reduction Initiatives

Some system managers went beyond existing Y2K requirements and employed further risk-reduction tactics.

Testing Vendor-Certified Products. Generally, system program managers rely on Y2K vendor certifications when purchasing Y2K upgrades and patches for noncompliant hardware and software.

Although the DoD Y2K Management Plan did not require that vendor-certified products be tested before system validation, a vendor-certified Y2K upgrade may fail during system validation, resulting in schedule delays, or a problem could remain hidden. To ensure that vendor-certified upgrades are Y2K compliant, it is prudent for program managers to test the upgrade before system validation.

In one case, the vendor-certified Y2K upgrade caused several system errors when processing post Y2K dates. The program manager for Personnel Concept III, an Air Force personnel system, purchased a $400,000 operating system upgrade to renovate the system's mid-tier noncompliant operating systems. The vendor stated that the operating system upgrade was Y2K compliant. The program manager tested the upgrade before system validation and found five instances in which post-2000 dates were processed incorrectly. After being notified by the system program manager, the vendor was correcting the upgrade by reviewing the discrepancies noted. Because the program manager identified the problem immediately, he had ample time to fix the upgrade before system validation and implementation was underway.

Ensuring Clients Are Compliant. Mid-tier systems generally employ a client-server relationship with the users of the system. In some cases, clients generate date-sensitive data to the host system's servers, incurring a potential risk that the clients may transmit noncompliant data and infect the entire system. Service and DoD guidance does not require system program managers to upgrade clients that the users own. However, in one instance, a program manager was taking positive action to ensure that all clients were Y2K compliant.

The Air Mobility Command Deployment Analysis System had 150 clients who use personal computers to transmit data to the host server. The system program manager was monitoring the status of all clients to ensure that they would be Y2K compliant. As of October 1998, 112 of the 150 users' personal computers were upgraded with compliant operating systems. The remaining 38 clients were scheduled to be upgraded by the end of December 1998. By monitoring the status of the clients, the system program manager was reducing the risk that noncompliant data generated from the users would infect the system servers.

Evaluating Discontinued Vendor Products. Mid-tier systems that use products for which the vendor discontinued support may experience integration problems when implementing Y2K replacement hardware and software. Some vendors abandon their hardware and software products rather than incurring the cost of creating Y2K-compliant upgrades and patches. Consequently, system program managers were forced to purchase new compliant software that might cause problems when integrating with existing system software. For example, the Functional Development Maintenance System used a critical software product that was assessed to be noncompliant. The vendor discontinued support for the software product but offered a Y2K-compliant replacement.

The program manager determined that the overall system operation would be adversely affected if the replacement product was implemented, assessed the probability of Y2K failure as "likely" using either product, and took positive action to develop a contingency plan specifically addressing the issue.

Summary

Managers of the mid-tier computer systems that we reviewed were aware of the Y2K status of each of the systems' primary elements and were actively engaged in ensuring the Y2K compliance of each element. Additionally, some system managers went beyond existing Y2K requirements and employed further risk-reduction tactics, such as testing vendor-certified Y2K products, ensuring that mid-tier clients are compliant, and evaluating discontinued vendor products. Accordingly, for the 14 mid-tier systems reviewed, we judged that the risk of system failure at the turn of the century from a primary element being overlooked was low. Furthermore, we strongly endorse the best practices discussed in this report.

Appendix A. Audit Process

This report is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the DoD Chief Information Officer to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at http://www.ignet.gov.

Scope

We reviewed Y2K reporting requirements and policies issued by the Office of the Secretary of Defense and the DoD Components. We discussed end-to-end testing plans with functional proponent officials. We reviewed DoD and DoD Component Y2K databases and held discussions with functional managers of various DoD Components to identify mid-tier computer systems and to identify any related concerns. We also interviewed managers of mid-tier computer systems and reviewed information on Y2K efforts and status to assess whether each major element of the computer system was adequately considered.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, DoD has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

- **Objective:** Prepare now for an uncertain future.
- **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities.

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Information Technology Management Functional Area.**
  Objective: Become a mission partner.
  Goal: Serve mission information users as customers.
- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer information needs.
  Goal: Modernize and integrate Defense information infrastructure.

- **Information Technology Management Functional Area.**
  Objective: Provide services that satisfy customer information needs.
  Goal: Upgrade technology base.

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from August through December 1998, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We used nonstatistical sampling methods, and we did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1997 and FY 1998 Annual Statements of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed at http://www.dodig.osd.mil.

Appendix B. Mid-Tier Systems Reviewed

We reviewed the following mid-tier systems from August through December 1998.

Air Mobility Command Development Analysis System. The Air Mobility Command Development Analysis System is the primary headquarters-level, mission-critical computer system for the Air Mobility Command, Scott Air Force Base, Illinois. The system provides planners and schedulers with the automated tools necessary to manage the extensive number of air mobility missions flown during peacetime, contingency, and humanitarian operations. The system has 142 mid-tier computers. It was completed on December 30, 1998.

Asset Management System. The Asset Management System is an Army transportation mission-critical system that automates the management of commercial containers within the Defense Freight Railway Interchange Fleet. The system maintains asset inventories at various Army transportation commands. It has four mid-tier computers and was implemented on October 30, 1998.

Drug and Alcohol Information System. The Drug and Alcohol Information System is a non-mission-critical system that is managed by the Program Executive Office – Standard Army Management Information Systems as part of the installation support modules. The system provides automated support for field-level tracking and managing the identification and rehabilitation of alcohol abusers and other drug abusers. The system is used to identify and track individuals throughout their enrollment in the Alcohol and Drug Abuse Prevention and Control Program. The system also provides installation commanders and other DoD policymakers with statistical information on alcohol and other drug abuse in the Army. The number of mid-tier computers associated with the system varies from site to site depending on the troop population. The system is in the renovation phase and is scheduled to be implemented by May 31, 1999.

Education Management Information System. The Education Management Information System automates each soldier's basic educational record to allow data entry, modification, query, and reporting at any installation. The system allows for electronic transfer and retrieval of records across DoD, tracks the soldier's academic progress, and ensures course compatibility. The number of mid-tier computers associated with the system varies from site to site depending on the troop population. The system is in the renovation phase and is scheduled to be implemented by May 31, 1999.

Functional Development Maintenance System. The Functional Development Maintenance System supports the functional development activities of personnel analysts who provide personnel data system support to Air Force base-level military personnel offices. The system is the primary development platform for the Base-Level Personnel System,

which provides quickly automated changes in personnel policies and procedures. The system has nine mid-tier computers in operation. It implemented on December 30, 1998.

Global Transportation Network. The Global Transportation Network is a mission-critical system that is headquartered at the U.S. Transportation Command, located at Scott Air Force Base, Illinois. Along with 24 interfacing systems, the Global Transportation Network provides data to track the movement of military assets in the air, over land, and across the sea. The system's primary function is to provide critical information on the location and status of people, cargo, and equipment. It has 50 mid-tier computers in operation. The system was completed on December 18, 1998.

Integrated Booking System. The Integrated Booking System is an Army transportation mission-critical system that provides a single, worldwide, automated booking system to support movement of unit and sustainment cargo. The system supports new traffic management business practices by automating the booking process between DoD shippers and ocean carriers. The system has four mid-tier computers in operation. It was implemented on October 30, 1998.

Integrated Command, Control, and Communications System. The Integrated Command, Control, and Communications System supports the Military Sealift Command's mission and feeds data to the Global Transportation Network. The system runs exclusively at the Washington Navy Yard and consists of seven command and control applications residing on a common platform. The system has one major mid-tier computer in operation. It was completed on December 31, 1998.

Keystone Retain. The Keystone Retain is an Army personnel mission-critical system that supports reenlistment, retention, reclassification, and Reserve component retention requirements for the Army. Keystone matches soldier qualifications with duty assignments and designates skill level 1 training. Keystone consists of four mid-tier computers. It is in the validation phase and is scheduled to be implemented by February 12, 1999.

Logistics Brokering System. The Logistics Brokering System is an Air Force transportation mission-critical system that provides connectivity for interfacing aircraft systems. The system routes aircraft status information by translating and reformatting passed data to the appropriate systems. The system has four mid-tier computers in operation. It is in the validation phase and is scheduled to be implemented by February 12, 1999.

Personnel Concept III. The Personnel Concept III is an Air Force personnel mission-critical distributed network information system designed to provide administrative and personnel support to commanders and their staffs worldwide. The system updates personnel information

and is administered by personnel system managers at base and civilian military flight stations. The system has 703 mid-tier computers fielded worldwide. It was completed on December 30, 1998.

Reserve Headquarters System. The Reserve Headquarters System is a mission-critical personnel system that collects and disseminates data necessary for the Commander of Naval Reserve Forces and upper echelon decisionmakers to manage selected Reserve mobilization and other strategic decisions. The system supports billet and mobilization management, incentive pay, unit and training management, automated modeling and projection of manpower assets or both, unit structuring, and unit siting. The system has three mid-tier computers in operation. It is in the validation phase and was scheduled to be implemented by January 22, 1999.

Reserve Standard Training Administration Readiness Support – Health Professionals. The Reserve Standard Training Administration Readiness Support – Health Professionals System supports the Navy Health Professionals Incentive Program requirements for both Active and Reserve forces. Navy organizations use the system to maintain personnel, enrollment, and stipend information. Specifically, the system collects and generates transactions for the Health Professionals Scholarship Program, the Financial Assistance Program, the Nurse Candidate Program, and the Special Training Assistance for Health Professionals Program. The system has one mid-tier computer. It was completed on December 30, 1998.

Source Data System. The Source Data System is a Navy personnel mission-critical system that automates local personnel functions and transmits the resulting data from field activities to the Navy corporate database. Regionally dispersed personnel support activities and their subordinate personnel support detachments use the system processing equipment, software, and interconnecting communications links to transfer data from the field activities within the continental United States, overseas, and shipboard units. The system has 49 mid-tier computers in operation. It is in the validation phase and is scheduled to be implemented by March 26, 1999.

Appendix C. Glossary

Application Program. An application program is a computer program to help people perform a certain type of work. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of those elements.

Computer Hardware. Computer hardware is the physical components of a computer system, including the mainframe processor, and peripherals, such as printers, tape silos, and direct access storage devices.

Defense Information Infrastructure - Common Operating Environment. The Defense Information Infrastructure - Common Operating Environment is the foundation for building open systems using a "plug and play" open architecture that is designed around a client-server model.

Mission-Critical Systems. Mission-critical systems include the following:

- systems defined by the Information Technology Management Reform Act (Clinger-Cohen Act) as National Security Systems (intelligence activities, cryptologic activities related to national security, command and control of military forces integral to a weapon or weapon system, or systems critical to direct fulfillment of military or intelligence missions);
- systems identified by the Commanders-in-Chief that, if not functional, would preclude the Commanders-in-Chief from conducting missions across the full spectrum of operations; and
- systems required to perform Department-level and DoD Component-level core functions.

Risk Assessment. A risk assessment is a continuous process performed during all phases of system development to provide an estimate of the damage, loss, or harm that could result from failure to successfully develop individual system components.

Testing. Testing consists of actions to determine whether the results generated by the information systems and their components are accurate and whether the systems perform to specifications.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Deputy - Y2K
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Army
Inspector General, Department of the Army
Auditor General, Department of the Army
Deputy Chief of Staff for Personnel
Director, Personnel Information Systems Directorate
Director, Military Traffic Management Command
Director, Program Executive Office, Standard Army Management Information Systems

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Navy
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps
Chief of Naval Personnel
Commander, Military Sealift Command
Commander, Navy Reserve Force
Director, Naval Reserve Information Systems Office

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force
Commander, Air Force Personnel Center
Director, Air Mobility Command

Unified Command

Commander in Chief, U.S. Transportation Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Chief Information Officer, General Services Administration
Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office
Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Governmental Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Thomas F. Gimble
Patricia A. Brannin
Mary Lu Ugone
James W. Hutchinson
Dan B. Convis
Hugh G. Cherry
Timothy J. Harris
Maria R. Palladino